1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld Bureau of Administration Information Sharing Services Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: October 9, 2009

(b) Name of system: Case Management System (DS)

(c) System acronym: CMS (DS)

(d) IT Asset Baseline (ITAB) number: 424

(e) System description (Briefly describe scope, purpose, and major functions):

Case Management System (CMS) is a client server application that was developed to support the tracking of security clearance requests and actions, investigations, and security and suitability adjudication. CMS tracks the investigation and adjudication of security clearance applications and suitability determinations for Department of State employees, prospective employees, and contractors; provides a means of recording individual Case files and Security files; provides a means of reporting based on criteria pre-defined by the user; provides a centralized repository for reference and tracking of background investigations for clearances.

(f) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security re-certification

(g) Explanation of modification (if applicable): Certification & Accreditation

(h) Date of previous PIA (if applicable): October 2, 2008

3. Characterization of the Information

The system:

☐ does NOT contain PII. If this is the case, you must only complete Section 13.

☒ does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

The information listed below is collected and maintained for the purpose of supporting the investigation and adjudication of security clearance applications.

- Name of an individual,
- Date and place of birth,

- Social security number,
- Gender,
- Height,
- Weight,
- Hair Color,
- Eye Color,
- Race,
- Naturalization Date (if applicable)
- Name and signature of spouse or cohabitant (if applicable)

This information is provided by Department of State employees, prospective employees, and contractors seeking a security clearance or a renewal of a security clearance. CMS collects and maintains information on Department of State employees, prospective employees, contractors, and their spouses, co-habitants, or domestic partners.

Spousal and cohabitant information may be collected as part of their spouse's or cohabitant's investigation. The Department may conduct a National Agency Check, without fingerprint cards, on an investigated individual's spouse or cohabitants. By definition, the National Agency Check consists of a review of:

(a) Investigative and criminal history files of the FBI;

(b) OPM's Security/Suitability Investigations Index (SII);

(c) DoD's Defense Clearance and Investigations Index (DCII);

(d) such other national agencies checks (e.g., Joint Personnel Adjudicative System (JPAS)) as appropriate to the individual's background.

b. How is the information collected?

The information collected and maintained by CMS is provided by Department of State employees, prospective employees, contractors, and their spouses, co-habitants, or domestic partners. This information is provided through the use of three separate forms, the SF-85 Questionnaire for Non-Sensitive Positions, SF-86 Questionnaire for National Security Positions and DS-7601 Authorization to Conduct Criminal History Inquiry for Spouse or Cohabitant. The SF-86 is completed online through e-QUIP and the SF-85 can either be completed and submitted electronically or manually completed and faxed to DSS/SI/PSS. The DS-7601 can be filled out electronically through eForms but it must be printed out and signed by the cohabitant or spouse. By signing the DS-7601 the spouse or cohabitant is verifying the accuracy of the information provided on the form and authorizing the Department of State to use this information for the purpose of conducting a criminal history inquiry. Once the DS-7601 is signed and completed it can either be sent via FEDEX, email, fax machine, or hand carried to DSS/SI/PSS. The method of delivery is determined by the spouse or cohabitant.

c. Why is the information collected and maintained?

Personally identifiable information is collected and maintained by CMS to support the tracking of security clearance requests. CMS and the information collected and maintained within CMS assists in the investigation and adjudication of security clearance applications for Department of State employees, prospective employees, and

contractors; provides a means of recording individual Case files and Security files; provides a means of reporting based on criteria pre-defined by the user; provides a centralized repository for reference and tracking of background investigations for clearances.

d. How will the information be checked for accuracy?

The agency or source providing the information is responsible for verifying accuracy. Specific methodologies for verification employed by Diplomatic Security (DS) include, among other things, maintaining the system as a live feed, allowing the information to be updated/edited at anytime, and cross referencing information with the DS/SI/PSS analyst or surrogates. Information found to be in error will be verified and updated by designated DS/SI/PSS Administrators.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

The legal authorities as documented in STATE-36, Diplomatic Security Records, specific to CMS, are as follows:

- Pub.L. 99-399 (Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended;
- Pub.L. 107-56 Stat.272, 10/26/2001 (USA PATRIOT Act); (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism); and
- Executive Order 13356, 8/27/04 (Strengthening the sharing of Terrorism Information to Protect Americans).

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

CMS collects the minimum amount of personally identifiable information necessary to assists in the investigation and adjudication of security clearance applications for Department of State employees, prospective employees, and contractors; provide a means of recording individual Case files and Security files; provide a means of reporting based on criteria pre-defined by the user; and provide a centralized repository for reference and tracking of background investigations for clearances.

There are numerous management, operational, and technical security controls in place to protect the data, in accordance with the Federal Information Security Management Act of 2002 and the information assurance standards published by the National Institute of Standards and Technology. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

The purpose of collecting select pieces of PII within CMS is to enable Diplomatic Security to track the status of pending and completed security clearance investigations.

b. What types of methods are used to analyze the data? What new information may be produced?

CMS provides DS/SI/PSS the ability to develop a matrix based on the status of security clearance investigations. Beyond this there is no new data produced by CMS.

Analysis of the information is limited to non-record metric-based statistical information, such as the number of cases entered, subject matter or action taken on an aggregate cycle (i.e., Monthly, Quarterly, Yearly, etc.).

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

CMS does not use commercial information, publicly available information, or information from other Federal agencies.

d. Is the system a contractor used and owned system?

CMS is a Government-owned system which was primarily designed and developed by contractors. All contractors have abided to regulatory guidelines and have signed and follow DS's Rules of Behavior.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

CMS does not create new information about the record subject. Thus, there are adequate safeguards in place to preserve data accuracy or integrity and avoid faulty determinations or false inferences about the record subject, thereby mitigating privacy risk. There is also no risk of "function creep," wherein with the passage of time PII is used for purposes for which the public was not given notice. Based on these specific uses that do not create additional information about the record subject, there is minimal privacy risk.

5. Retention

a. How long is information retained?

The retention period of data is consistent with established Department of State policies and guidelines as documented in the Department of State's Disposition Schedule of Diplomatic Security Records, Chapter 11.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

CMS collects and maintains names, date and places of birth, social security numbers, gender, height, weight, hair color, eye color, race, and naturalization date on Department of State employees, prospective employees, and contractors seeking a security clearance or a renewal of a security clearance and their spouse, co-habitant, or domestic partner. There are inherent risks associated it these types of information. In an attempt to mitigate these risks the Department of State has implemented numerous management, operational and technical security controls in order to protect the information in accordance with the Federal Information Security Management Act of 2002 and the information assurance standards published by the National Institute of Standards and Technology. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security identification and authentication, contingency planning, media handling, configuration

management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software) and audit reports.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

Limited access is granted to Security Officers (SO) throughout the Department of State. With this limited access SOs are allowed to view names, dates and places of birth, social security numbers, height, weight, hair color, and eye color. The purpose of providing this limited access to SOs is to allow the SO to verify the clearance level of an individual.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

The information collected and maintained by CMS is shared throughout the Department through limited access controls. Numerous management, operational and technical controls are in place to reduce and mitigate the risks associate with internal sharing and disclosure including, but not limited to annual security training, separation of duties, least privilege and personnel screening.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

It is possible for an employee with authorized access working for the Department of State to use his or her access to this information to retrieve PII on an individual and use this information in an unauthorized manner. In order to mitigate this risk all Department employees are required to undergo computer security and privacy awareness training prior to accessing CMS, through which the information is shared, and must complete refresher training yearly in order to retain access.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

The information collected and maintained within CMS is shared with the Office of Personnel Management (OPM) through the Clearance Verification System (CVS). The purpose of sharing this information is to allow other government agencies to validate the clearance of DoS employees.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Safeguards in place: CMS is monitored and guided by the inherited security controls of the OpenNet. Controls built into the OpenNet General Support System (GSS), including routers and Network Intrusion Detection System (NIDS); provide network level controls that limit the risk of unauthorized access from all IP segments, to include patch management, configuration management, and segregation of duties.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

The risks associated with sharing privacy information externally and the disclosure of privacy information is generally higher than internal sharing and disclosure. Intentional and unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. Transmission of privacy data in an unencrypted form (plain text), and use of not secure connections are also a serious threat to external sharing. Numerous management, operational and technical controls are in place to reduce and mitigate the risks associate with external sharing and disclosure including, but not limited to formal Memorandums of Agreement/Understandings (MOA/MOU), service level agreements (SLA) annual security training, separation of duties, least privilege and personnel screening.

8. Notice

The system:

☒ Contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records.

(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems):

STATE-36 Information Access Programs Records

☐ Does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Notice of the purpose, use and authority for collection of information submitted are described in the System of Records Notices titled STATE-36.

Additionally a Privacy Act Statement is included on forms SF-86, SF-85, and DS-7601 used to collect information for CMS. The Privacy Act Notice is included at the bottom of the form and by signing this form the employee, contractor, spouse or cohabitant is verifying his or her understanding that the information will be used for the purpose of conducting a criminal history inquiry.

b. Do individuals have the opportunity and/or right to decline to provide information?

The individual is informed of the Privacy Act statement; whereby, the acknowledgement of the Privacy Act notice signifies the individual's consent to the use of his or her information. Notice of the purpose, use and authority for collection of information submitted are also described in the System of Records Notice titled STATE-36.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No. The utility of the information in the system about a particular individual will not extend over the allotted time in the Department of State's Disposition of Schedule, as defined in Diplomatic Security Records, Chapter 11. Moreover, there is negligible

privacy risk as a result of degradation of its information quality over an extended period of time.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The notice offered is reasonable and adequate in relation to the system's purposes and uses.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

CMS contains Privacy Act-covered records; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the system of records notice identified in paragraph 8 above, and in rules published at 22 CFR 171.31. The procedures inform the individual about how to inquire about the existence of records about them, how to request access to their records, and how to request amendment of their record. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of a passport records on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

The Business Owner DS/P/PL approves and authorizes use of the CMS system. System accounts are maintained and reviewed on a regular basis. The following DoS policies establish the requirements for access enforcement.

- 5 FAM 731 SYSTEM SECURITY (Department computer security policies apply to Web servers)
- 12 FAM 622.1-2 System Access Control
- 12 FAM 623.2-1 Access Controls
- 12 FAM 629.2-1 System Access Control
- 12 FAM 629.3-3 Access Controls

The database enforces a limit of 3 consecutive invalid access attempts by a user during a 15 minute time frame. After 20 minutes of inactivity a session lock control is implemented at the network layer.

The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. The level of access for the user restricts the data that may be seen and the degree to which data may be modified. A system use notification ("warning banner") is displayed before log-on is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

Non-production uses (e.g., testing, training) of production data are limited by administrative controls.

Diplomatic Security uses an array of configuration auditing and vulnerability scanning tools and techniques to periodically monitor the OpenNet-connected systems that host DS's major and minor applications, including the CMS components, for changes to the DoS mandated security controls.

b. What privacy orientation or training for the system is provided authorized users?

All users are required to undergo Cyber Security Training which encompasses computer security and privacy awareness, prior to accessing the system, and must complete refresher training yearly in order to retain access. In addition, users are required to sign a user agreement stating that they understand they are not allowed to use CMS and the information contained within for any purpose that may be other than official.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system generates audit trails which can be analyzed and reviewed in the event that misuse of the system is suspected. (An audit trail provides a record of which particular functions a particular user performed, or attempted to perform on an information system.)

11. Technologies

a. What technologies are used in the system that involves privacy risk?

All hardware, software, middleware, and firmware are vulnerable to risk. There are numerous management, operational, and technical controls in place to mitigate these risks. Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database (NVD), following and implementing sound federal, state, local, department and agency policies and procedures are only a few of the safeguards implemented to mitigate the risk to any Information Technology. CMS has been designed to minimize risk to privacy data.

Moreover, the method of transmission chosen by the spouse or cohabitant has the potential to expose his or her PII to risk. While the Department of State cannot secure communications beyond its boundaries of ownership it has taken steps to mitigate risk to the PII within its control. These steps include limiting access to group email accounts where forms like the SF-85 might be emailed too and providing all Department of State employees training on the proper handling procedures of Privacy Act related information.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

All hardware, software, middleware and firmware are vulnerable to risk. There is numerous management, operational, and technical controls in place to mitigate these risks. Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database (NVD), following and implementing sound federal, state, local, department and agency policies and procedures are only a few of safeguards implemented to mitigate the risks to any Information Technology.

12. Security

What is the security certification and accreditation (C&A) status of the system?

CMS is part of the DoS Clearance ATO, which was approved in May of 2007.